(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－297541
（P2002－297541A）
(43)公開日　平成14年10月11日(2002.10.11)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ａ　５Ｂ０８５
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ａ　５Ｊ１０４
			６４０Ｄ

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願2001－102393(P2001－102393)

(22)出願日　平成13年３月30日(2001.3.30)

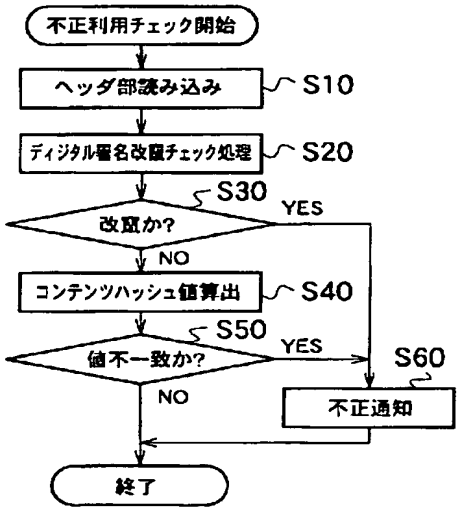
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　黒川　清
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　東　正造
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　不正利用通知方法、不正利用通知装置および不正利用通知プログラム

(57)【要約】
【課題】　本発明は、クライアント側で自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる不正利用通知方法、不正利用通知装置および不正利用通知プログラムを提供することにある。
【解決手段】　流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出し（Ｓ１０）、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出（Ｓ４０）しておき、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断（Ｓ５０）し、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信（ステップＳ６０）する。

不正利用チェックフロー



1

【特許請求の範囲】

【請求項１】　配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知方法であって、
流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、
流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、
流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、
不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを特徴とする不正利用通知方法。

【請求項２】　配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知装置であって、
流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出手段と、
流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出手段と、
流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断手段と、
不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信手段とを有することを特徴とする不正利用通知装置。

【請求項３】　配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知プログラムであって、
流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、
流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、
流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、
不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを特徴とする不正利用通知プログラム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、広範に流通するコンテンツの流通監視を行い、不正利用を検出して不正利用情報を通知する不正利用通知方法および不正利用通知装置に関する。

【０００２】

【従来の技術】従来の不正利用通知方法としては、電子透かし技術を用いてコンテンツを一意に識別できるコンテンツＩＤなどを予めコンテンツに埋め込でおいて流通させ、不正利用検出システムにより、正規配布先のＵＲＬと埋め込んだコンテンツＩＤとの対応関係をチェックして不正利用を監視するというネットポリス技術が知られている。

【０００３】このような不正利用検出システムにおいて用いられている検出技術としては、以下の技術が知られている。

【０００４】（１）透かし読み取り機能を有する探索ロボットにより、Ｗｅｂサイトのページに含まれているコンテンツをトップダウン的に探索する技術。

【０００５】（２）特定ネットワークに設けられた特定ノードのゲートウェーやサーバに透かし読み取りフィルタを組み込んでおき、このフィルタを通過するコンテンツを全てチェックする技術。

【０００６】（３）利用者のブラウザのダウンロードモジュールに透かし読み取りツールを予めプラグインしておき、ＷｅｂサーバからダウンロードしたコンテンツのコンテンツＩＤとアクセスサイトのＵＲＬをコンテンツＩＤ管理センタに通知してチェックする、ボトムアップ的な利用者協力型がある。

【０００７】例えば、エム研（http://www.mken.co.jp/）では、以下のようなサービスを行っている。

【０００８】このサービスでは、透かし検知ロボットにより、透かし入りコンテンツに関連しそうな単語をキーワードとしてサーチエンジンでピックアップしたＷｅｂサイトを中心に回るイエローリスト巡回方式と、著作権違反の可能性のあるコンテンツを持っているＷｅｂサイトを中心に回るグレーリスト巡回方式とに従って２４時間常時インターネットを監視しており、世界中のホームページを巡回して例えば、「acuaporta 」の電子透かしを埋め込んだコンテンツをデコードして監視し、不正にコピー、改竄されてネットワーク上に掲示されたコンテンツの発見に努めている。

【０００９】

【発明が解決しようとする課題】このように、従来の不正利用通知方法では、著作権保護技術によりカプセル化を行い、専用のソフトを利用して、鍵・利用条件・クライアント情報などの認証を行うことにより不正利用を防止していた。また、管理サーバに不正利用の疑いのあるコンテンツを転送し、コンテンツに予め埋め込んである

電子透かしなどを検出していた。

【００１０】しかしながら、従来の不正利用通知方法にあっては、管理サーバに不正利用の疑いのあるコンテンツを持ち込む必要があるので、インターネットの普及に伴って管理サーバの稼動負荷が増大するとともに、管理サーバの増設が必要になるといった問題があった。

【００１１】そこで、管理サーバの稼動負荷の増大や管理サーバの増設などを行なわずに、コンテンツを再生するクライアント側のメディアプレイヤに不正利用を検出して通知する方法が求められてきた。

【００１２】本発明は、上記に鑑みてなされたもので、その目的としては、クライアント側で自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる不正利用通知方法、不正利用通知装置および不正利用通知装置を提供することにある。

【００１３】

【課題を解決するための手段】請求項１記載の発明は、上記課題を解決するため、配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知方法であって、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを要旨とする。

【００１４】請求項２記載の発明は、上記課題を解決するため、配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知装置であって、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出手段と、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出手段と、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断手段と、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信手段とを有することを要旨とする。

【００１５】請求項３記載の発明は、上記課題を解決するため、配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知プログラムであって、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを要旨とする。

【００１６】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【００１７】図１は、本発明の一実施の形態に係る不正利用通知方法を適用可能なＤＲＭ処理フローの構成を示す図である。

【００１８】図１に示すように、本システムには、コンテンツを作成するためのエンコーダ装置１３、コンテンツを管理するためのＤＲＭ（Digital Rights Management）装置１７、コンテンツを配信するためのメディアサーバ２１、コンテンツを再生するためのメディアプレイヤ２３が設けられている。

【００１９】エンコーダ装置１３は、一般に符号器と呼ばれ、カメラからのライブ画像、マルチメディアファイル、クライアント（パーソナルコンピュータ）の画面情報などのメディアファイルＡ１１を入力して一定の規則に従って符号化して指定形式の圧縮されたファイルに変換する機能を有しており、変換されたメディアファイルＢ１５が出力される。

【００２０】ＤＲＭ装置１７は、Ｗｅｂサーバからなり、Ｗｅｂサイトのメニューページや、情報の要求または支払いが行われる登録ページを提供して、登録ページ上から解凍のためのライセンスキーなどを与える機能を有している。特に、ＤＲＭ装置１７は、コンテンツを保護するためのライセンス管理や著作権管理機能によりコンテンツ管理を行っており、エンコーダ装置１３により変換されたメディアファイルＢ１５を入力して鍵番号とライセンスを取得するためのＵＲＬ情報を付加し、メディアファイルＢ１５に対して、エンコーダ装置１３による変換の逆変換を行うことが可能な鍵番号とライセンス取得ＵＲＬ情報を用いて暗号化して一体のデータになるようにカプセル化し、このカプセル化されたメディアファイルＣ１９をメディアサーバ２１に送信する。なお、カプセル化されたメディアファイル１９は、ライセンスとともに暗号化され「鍵」を用いなければ上述した逆変換が不可能なように保護されている。この「鍵」は、ＤＲＭ装置１７からメディアプレイヤ２３に別途配布される。

【００２１】また、カプセル化されたメディアファイル

１９を利用者にダウンロードさせるためにサーバ上のＷｅｂサイトに置いたり、ストリーミングのためにメディアサーバ２１上に置いたり、ＣＤ－ＲＯＭを媒体として配布したりする。

【００２２】メディアプレイヤ２３は、ＤＲＭ装置１７との通信機能をサポートしており、例えば、メディアサーバ２１からカプセル化されたメディアファイルＣ１９をダウンロードし、メディアファイルＣ１９から抽出した鍵番号とコンテンツＩＤを抽出してＤＲＭ装置１７に送信し、ＤＲＭ装置１７からこの鍵番号とコンテンツＩＤに対応する鍵と利用条件およびクライアント情報などの証明書が返信され、カプセル化されたメディアファイルＣ１９がメディアファイル２５に逆変換され、ライセンスに含まれている利用条件に従ってメディアファイル２５がデコード機能により再生される。なお、ライセンスには、開始時刻、日付、期間、再生回数などのさまざまな権利行使するための利用条件を与えることができる。

【００２３】また、保護されたメディアファイルＣ１９を再生するためには、利用者はまずメディアファイルＣ１９をメディアファイルＢ１５に逆変換するためのライセンスキーを取得する必要がある。ライセンスキーの取得タイミングは、利用者が保護されたメディアコンテンツＣ１９を取得しようと試みたときや、メディアファイルを初めて再生したときに自動的に開始される。

【００２４】このときＤＲＭ装置１７は、Ｗｅｂサイトのメニューページから情報の要求または支払いが行われるＷｅｂサイト上の登録ページに利用者を誘導し、利用者は誘導された登録ページ上から解凍のためのライセンスキーを取得することとなる。

【００２５】また、メディアプレイヤ２３は、メディアファイルＣ１９を再生中に、このメディアプレイヤ２３が存在するクライアント（パーソナルコンピュータ）上のコンテンツＩＤに準拠したメディアファイルを順次参照して、後述する不正利用チェックフローによりのメディアファイルの不正利用があるかどうかを確認する。

【００２６】次に、図２は、コンテンツＩＤの詳細な構成に示す説明図である。

【００２７】詳しくは、図２に示すように、コンテンツＩＤには、コンテンツに関する属性情報を特定するためにコンテンツに一意的に付与される識別子として、左側から、コンテンツに一意に付与される番号（ユニークコード）を表すＩＤセンタ管理番号、コンテンツのクリエータや内容や種別や分類などに関する情報を表すコンテンツ属性、コンテンツの権利関係を表記する権利属性、権利の許諾・選任・確認に関する情報を表す権利運用属性、コンテンツの流通（＝売買）の履歴情報を表す流通属性、売買収益の分配に関する情報を表す分配属性、ＩＤ管理センタに任される自由領域を表す自由領域、ディジタル署名やコンテンツハッシュ値などを表すシステム

領域などが設定されている。

【００２８】さらに、コンテンツＩＤの構成要素には、コンテンツを特定するための情報と流通に関する情報、電子透かしの方式などシステムに関する情報がある。これらの表現方法には、ユニークコード、流通記述子（ＤＣＤ：Distributed ContentDescription ）があり、必要に応じて使い分ける。なお、流通記述子（ＤＣＤ）は、コンテンツＩＤの中で権利者により予め規定された利用条件などの重要情報である。

【００２９】このうち、システム領域には、図３に示すように、コンテンツとコンテンツＩＤ（流通記述子：ＤＣＤ）をバンドルするためのディジタル署名とコンテンツハッシュ値が含まれており、これらを利用して不正チェックを行う。さらに、システム領域には、コンテンツデータと連結するためのコンテンツへのリンク、電子透かし情報、署名アルゴリズム情報、チェックディジットなどがある。

【００３０】ここで、ディジタル署名とコンテンツハッシュ値のデータ構造や数理的特徴を説明し、不正チェックをどのように行うかを説明する。

【００３１】図３に示すように、公開鍵暗号方式に基づいたデジタル署名においては、署名作成者がその通信内容となるコンテンツ（電子文書）を署名者固有の署名鍵（秘密鍵）により暗号化し、署名付きコンテンツ（電子文書）の受信者がその署名鍵に対応する署名作成者の検証鍵（公開鍵）によりそのデジタル署名が本当に送信者の署名であるのかどうかを検証することができるという仕組みになっている。

【００３２】従って、デジタル署名は、通信内容を暗号化したものを署名とするという技術的な特性から、署名そのものと通信内容である電子文書自体との結合性が強く、もし通信内容が通信途上で改竄されれば、後述する署名の検証過程によって、改竄されたという事実も検証することができるという利点がある。

【００３３】具体的な実現方法の１つであるクリアディジタル署名（分離署名）は、図３に示すように、コンテンツデータとディジタル署名が分離されており、コンテンツデータはそのまま読め、一方、ディジタル署名が記述されているシステム領域には、コンテンツ本文のコンテンツハッシュ値（秘密の計算式で計算した値）を含んでいる。

【００３４】このため、ディジタル署名が改竄された場合には、ディジタル署名の署名対象となるコンテンツハッシュ値も同時に改竄されることになる。その結果、実際のコンテンツハッシュ値を計算して、計算されたコンテンツハッシュ値とコンテンツＩＤ中のコンテンツハッシュ値が異なり、ディジタル署名の改竄を検出することができる。

【００３５】ここで、図３に示すコンテンツハッシュ値は、予め決められたハッシュ関数により得られた値であ

り、ハッシュ関数には、不可逆な一方向関数を含むため、コンテンツハッシュ値からコンテンツデータを再現することはできず、また同じコンテンツハッシュ値を持つ異なるコンテンツデータを作成することは極めて困難である。なお、ハッシュ関数としては、例えば、ＭＤ５、ＳＨＡ１などが広く知られている。

【００３６】また、具体的な検出過程では、このハッシュ関数は、与えられたコンテンツデータから固定長の疑似乱数を生成する演算手法であり、通信などの流通過程を通じてコンテンツデータを提供する際に、流通前のコンテンツデータからハッシュ関数を用いて求めておいたコンテンツハッシュ値をコンテンツＩＤのシステム領域から抽出しておき、流通後のコンテンツデータからハッシュ関数を用いて求めたコンテンツハッシュ値と比較すれば、コンテンツデータが通信などの流通途中で改竄されているかどうかを調べることができる。

【００３７】次に、図４は、コンテンツの作成時におけるコンテンツＩＤの埋め込みフローである。

【００３８】図４に示すように、メディアファイルＡ１１として、音声ファイルに関してＷＡＶ．ＷＭＡ．ＭＰ３などの識別子があり、映像ファイルに関してＷＭＶ．ＡＳＦ．ＡＶＬ．ＭＰＥＧ１などの識別子があり、その他のファイルの識別子としてＢＭＰがある。メディアファイルＡ１１は、二階層電子透かしをオプションとして扱うことができる。

【００３９】エンコーダ装置１３で変換されたメディアファイルＢ１５として、ＷＭＡ，ＷＭＶ，ＡＳＦなどの識別子があり、これらのカプセル化されたメディアファイルＢ１５のヘッダ情報へ上述したＤＣＤを埋め込む。

【００４０】ＤＲＭ装置１７でカプセル化されたメディアファイルＣ１９は、上述したＤＣＤをバインドする。

【００４１】なお、メディアファイルＡ１１は、ＩＤセンタ管理番号からなるユニークコードを用いた二階層電子透かしをオプションとして扱うことができる。

【００４２】ここで、二種類の異なる電子透かしを順次埋め込む二階層電子透かしについて説明する。

【００４３】電子透かしには、多数の方式があり、すべての電子透かしを順次試みるとなると、検出時間が膨大になってしまう恐れがあるため、メタ電子透かしを用いて実電子透かしの種別情報を埋め込むようにする。この実電子透かしは、ＩＤセンタの管理番号を埋め込むものであり、メタ電子透かしは、実透かしの種別情報を埋め込むものである。

【００４４】検出手順は、メタ電子透かしの検出により実電子透かしの種別を特定し、さらに、特定した実透かしを検出するようにするので、二種類の異なる電子透かしにより埋め込まれたユニークコードの検出過程を複雑化でき、不正利用者による容易な解読をできないようにすることができる。

【００４５】なお、ユニークコードは、ＩＤセンタ管理

番号を示しており、その構成は以下の通りである。

【００４６】（１）地域コード（4bit）
世界を１６地域に分割してセンタの番号付与が可能である。

【００４７】（２）センタ番号（8bit）
Registoration Authority が発行し、ＩＤセンタを識別する固定長の番号である。

【００４８】（３）センタ内番号（任意）
ＩＤセンタが管理するコンテンツを識別する番号であり、ＩＤセンタが任意に割付ける。

【００４９】（４）バージョン番号（4bit）
コンテンツＩＤのバージョンを２進数によるバイナリ表現を用いて規定した番号である。

【００５０】次に、図５は、メディアプレイヤ２３の機能構成を示す図である。

【００５１】メディアプレイヤ２３は、メディアファイル２５の再生中に、メディアプレイヤ２３が存在するクライアント上のコンテンツＩＤに準拠したファイルを順次チェックし、不正利用のメディアファイルを確認する。

【００５２】図５に、メディアプレイヤ２３の機能構成の一例を示す。メディアプレイヤ２３は、認証部４１、流通情報蓄積部４３、不正利用チェック部４５、メディア再生部４７から構成されている。

【００５３】また、メディアプレイヤ２３により再生されるメディアファイルは、先頭からヘッダ情報、システム化領域、ディジタル署名、コンテンツハッシュ値、コンテンツ領域を有している。

【００５４】認証部４１は、入力されたメディアファイルから鍵番号とコンテンツＩＤを抽出してＤＲＭ装置１７に送信し、ＤＲＭ装置１７から鍵・利用条件・クライアント情報などの証明書を受信して認証を行う。

【００５５】流通情報蓄積部４３は、過去に再生したメディアファイルのコンテンツＩＤから収集した流通属性を流通情報として蓄積する。

【００５６】不正利用チェック部４５は、クライアント上のメディアファイルをサーチし不正利用を検出するモジュールであり、その詳細な動作を図６に示す不正利用チェックフローにより処理される。

【００５７】メディア再生部４７は、ＤＲＭ装置１７から受信した利用条件に従ってメディアファイル２５をデコード機能により再生する。このデコード機能は、エンコーダ装置１３による符号化とは逆に、符号化されたメディアファイル２５をメディアファイルＡ１１に復号する機能である。

【００５８】ここで、図５に示すメディアプレイヤ２３での基本的な動作を説明する。

【００５９】なお、パーソナルコンピュータからなるクライアントには、制御部にＯＳプログラムや制御データやアプリケーションプログラムを一時的に記憶するＲＡ

Ｍと、制御プログラムやアプリケーションプログラムに従ってシステムを制御するＣＰＵとが設けられている。また、ハードディスクＨＤに記録されているアプリケーションプログラムは、例えばパーソナルコンピュータに設けられたＣＤ－ＲＯＭドライブなどを用いてＣＤ－ＲＯＭなどの記録媒体からインストールされたプログラムであり、本発明の不正利用通知プログラムを記録した記録媒体などである。

【００６０】クライアント上でメディアプレイヤ２３の画面からメディアサーバ２１のＵＲＬを指定してホームページを開き、メディアファイルを受信する。そして、認証部４１では、入力されたメディアファイルから鍵番号とコンテンツＩＤを抽出してＤＲＭ装置１７に送信する。そして、認証部４１が、ＤＲＭ装置１７から鍵・利用条件・クライアント情報などの証明書を受信して認証を行う。そして、メディア再生部４７では、メディアファイル２５をＤＲＭ装置１７から受信した開始時刻、日付、期間、再生回数などの利用条件に従ってメディアファイルＡ１１に復号して再生する。

【００６１】このメディア再生部４７でメディアファイルの再生を行っている際に、並行して不正利用チェック部４５は、バックグラウンドでクライアント上にある他のメディアファイルを対象にした不正利用チェックを行う。

【００６２】図６において、不正利用チェックを開始すると、ステップＳ１０では、メディアファイル２５のコンテンツＩＤからヘッダ情報を読み込み、特に、流通後のメディアファイルに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値とディジタル署名を読み出す。

【００６３】そして、ステップＳ２０では、ディジタル署名の改竄チェック処理を行う。

【００６４】すなわち、流通前に記述されたコンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いて流通後のコンテンツハッシュ値を計算して、計算された流通後のコンテンツハッシュ値とコンテンツＩＤ中に記述されている流通前のコンテンツハッシュ値が異なった場合には、ディジタル署名の改竄があったこととなる。

【００６５】そして、ステップＳ３０では、改竄があるかどうかを判断する。改竄がない場合には、ステップＳ４０に進み、流通後のコンテンツに対して流通前に記述されたコンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いて流通後のコンテンツハッシュ値を算出する。

【００６６】そして、ステップＳ５０では、算出した流通後のコンテンツハッシュ値がメディアファイル２５のコンテンツＩＤから読み出した流通前のコンテンツハッシュ値と不一致かどうか判断する。

【００６７】ここで、算出した流通後のコンテンツハッシュ値がメディアファイル２５の流通前のコンテンツハッシュ値と一致した場合には、正常な利用であることを示しているので、そのまま処理を終了する。

【００６８】一方、ステップＳ３０で改竄があると判断した場合、または、ステップＳ５０で流通前後のコンテンツハッシュ値同士が不一致の場合、ステップＳ６０に進み、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信し、処理を終了する。

【００６９】このように、不正利用チェック部４５において、メディアファイル２５のディジタル署名とコンテンツハッシュ値の確認を行うので、当該メディアファイル２５が不正利用かどうかを検出することができ、当該メディアファイル２５が不正利用の場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信することができる。

【００７０】また、コンテンツＩＤに示されるセンタアドレス（センタサーバのＵＲＬ）に、不正利用があったことを示す不正利用情報を通知することができる。なお、この不正利用情報には、コンテンツＩＤと存在場所（端末のＩＰアドレス）、不正利用チェック結果を含むこととする。

【００７１】この結果、自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができ、特に、メディアプレイヤに適用することができる。また、クライアント側の不正監視手段として適用することができる。

【００７２】また、メディアプレイヤのバージョンアップに合せて、新しいディジタル署名方式や新規チェック項目を追加した場合でも、不正利用検出フローを容易に改定することができる。

【００７３】本実施の形態における効果は、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出し、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出しておき、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断し、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信することで、自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる。

【００７４】

【発明の効果】請求項１乃至３記載の本発明によれば、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出し、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と

11

同一のハッシュ関数を用いてコンテンツハッシュ値を算出しておき、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断し、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信することで、自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係る不正利用通知方法を適用可能なＤＲＭ処理フローの構成を示す図である。

【図２】コンテンツＩＤの詳細な構成に示す説明図である。

【図３】ＤＣＤの詳細な構成に示す説明図である。

【図４】コンテンツ作成時のコンテンツＩＤの埋め込みフローである。

12

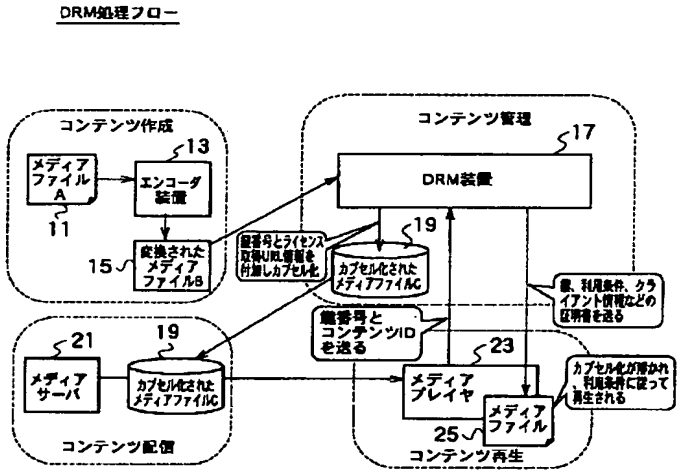
【図５】メディアプレイヤ２３の機能構成を示す図である。

【図６】不正利用チェック部４５の詳細な動作を説明するためのフローである。

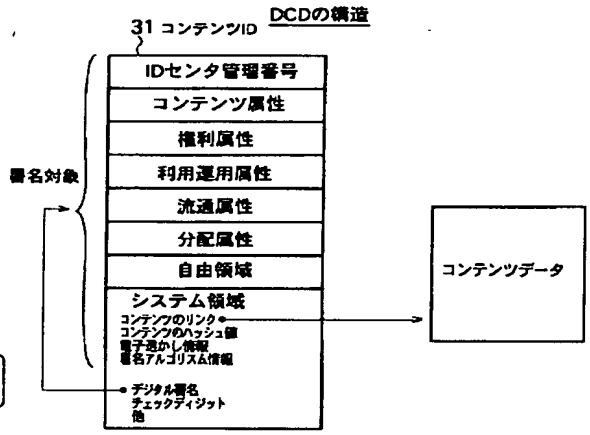
【符号の説明】

１３　エンコーダ装置
１７　ＤＲＭ装置１７
２１　メディアサーバ
２３　メディアプレイヤ
２５　メディアファイル
３１　コンテンツＩＤ
４１　認証部
４３　流通情報蓄積部
４５　不正利用チェック部
４７　メディア再生部

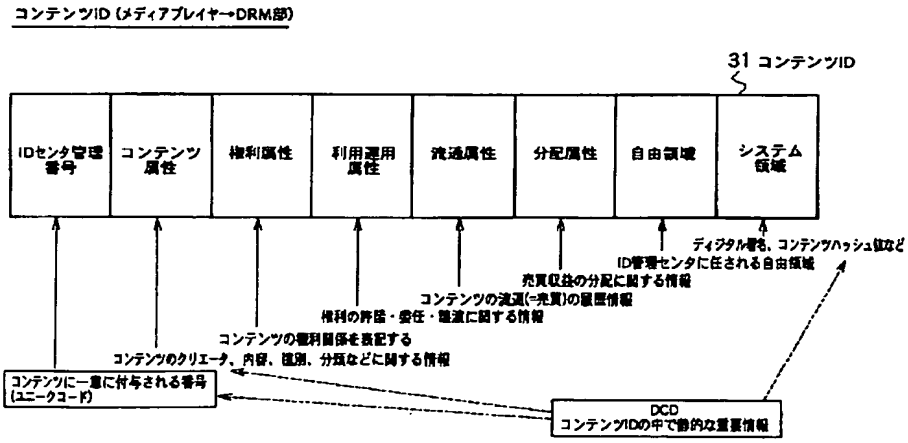
【図１】



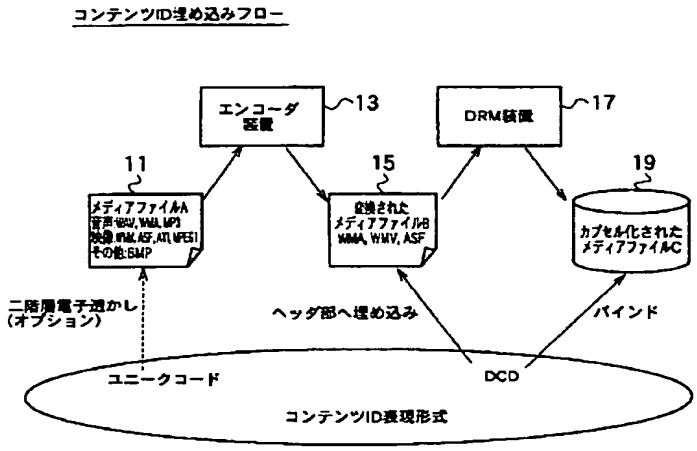
【図３】



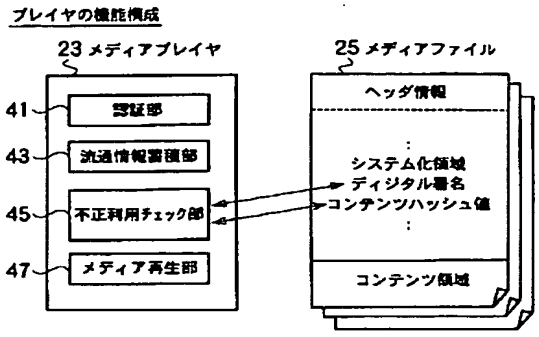
【図２】



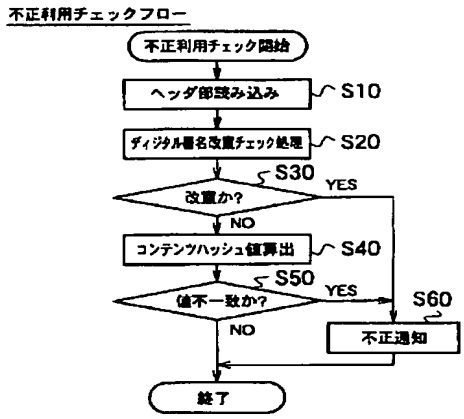
【図４】



【図５】



【図６】



フロントページの続き

(72)発明者　佐野　睦夫
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B085 AE00
5J104 AA08 AA13 LA02 LA05 NA12 PA14

拒絶理由通知書

特許出願の番号	特願２００２－３２１３５９
起案日	平成１８年　７月３１日
特許庁審査官	高野　美帆子　　９８４９　５Ｑ００
特許出願人代理人	杉浦　正知（外　１名）　様
適用条文	第２９条第２項、第３６条

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

理由１

この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　　（引用文献等については引用文献等一覧参照）

・請求項　１－８，１０－１３，１６－１７，１９－２４，２６－３０，３２
・引用例　１－２
・備考

引用例１には、ＲＯＭ領域にコンテンツデータが記録された媒体の媒体識別情報と媒体の管理情報とを関連づけてサーバに記憶させ、記録媒体に記録された媒体識別情報を読み出してネットワークを介して送信し、受信された媒体識別情報から媒体の管理情報を読み出して管理情報に基づいてコンテンツの再生を可能にする鍵を発行してネットワークを介して端末側に送信し、管理情報に応じたサービスを提供し、利用形態に応じて管理情報を書き換えるシステムについて記載されており、管理情報は利用可能情報（再生条件）である再生可能回数及び再生有効期限を含み、利用可能情報（再生条件）はディスク販売時（ユーザに入手される時）に設定可能であることについても記載されている。

引用例２には、暗号化された超流通コンテンツの著作権管理に関して、コンテンツをＲＯＭメディアで提供する技術、著作権管理を再生又は他の媒体へのコピーの制御において行う技術、再生かコピー（買い取り）かの利用形態を示す課金情報を送信する技術について記載されている。

引用例１と２は共にコンテンツの著作権管理に関する共通の技術分野に属する。

したがって、本願請求項１－８，１０－１３，１６－１７，１９－２４，２６

－３０，３２に係る発明は、引用例１に記載された発明に、引用例２のＲＯＭメディアで提供する技術、再生だけではなくコピー制御の著作権管理をする技術、利用形態も送信する技術を必要に応じてそれぞれ適用し、当業者が容易に成し得たものである。

・請求項　９，１８，２５，３１
・引用例　１－４
・備考
　引用例３の第００２０段落又は引用例４の００２２段落には、鍵データにコンテンツに対する利用権情報を付加して送信する技術について記載されている。
　引用例１－４は全てコンテンツの著作権管理に関する共通の技術分野に属する。
　したがって、本願請求項９，１８，２５，３１に係る発明は、引用例１に記載の発明において鍵データを送信する際に、引用例３又は引用例４の鍵データに利用権を付加して送信する技術を適用し、必要に応じて引用例２に記載されたそれぞれの技術を適宜、引用例１に適用し、当業者が容易に成し得るものである。

・請求項　１４－１５
・引用例　１，５
・備考
　引用例１には、媒体購入時に利用権（再生条件）を設定する技術と、さらに、利用権を媒体識別情報と共にサーバに送信する技術についても記載されている。
　また、利用権を媒体購入時に設定する際に、媒体購入店における端末を使用するようにすることは、当業者であれば適宜設計可能な事項である。
　引用例５には、ＲＯＭメディア購入時に店舗端末を使って媒体ＩＤをサーバに送信する技術について記載されている。（第９頁第３８行目－第４４行目参照）
　引用例１，５は共にコンテンツの著作権管理に関する共通の技術分野に属する。
　したがって、本願請求項１４－１５に係る発明は、引用例１の媒体入手時に、引用例５のＲＯＭ媒体入手時に店舗端末から媒体識別情報をサーバに送信する技術を適用し、当業者が容易に成し得たものである。

引　用　文　献　等　一　覧
１．特開２００２－２９７４５３号公報
２．特開２０００－１９６５８５号公報
３．特開２００１－２０９５８６号公報

４．特開２００２－２９７５４１号公報
５．国際公開第０２／０５２４７３号

理由２
　この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第２号に規定する要件を満たしていない。

記

・請求項　６

・備考
「該利用の形態」と記載されているが、利用の形態は前記されておらず、どの利用の形態を指しているのかわからない。

・請求項　２６－３２
・備考
「再生および／または記録制御装置」との記載は、再生制御装置、記録制御装置、記録再生制御装置のうち、どの制御装置の発明と特定してよいのかわからない。
よって、請求項６，２６－３２に係る発明は明確でない。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

先行技術文献調査結果の記録

・調査した分野　　ＩＰＣ第７版　Ｇ１１Ｂ２０／１０
Ｇ０６Ｆ１２／１４
Ｇ０６Ｆ　３／０６
Ｈ０４Ｌ　９／００

この先行技術文献調査結果の記録は、拒絶理由を構成するものではありません。

この拒絶理由通知の内容に関するお問い合わせ、または面接のご希望がございましたら下記までご連絡下さい。

特許審査第四部データ記録　高野　美帆子
TEL. 03(3581)1101 内線3589～3591
FAX. 03(3580)6906

部長／代理	審査長／代理	審査官	審査官補
	渡邊　聡	高野　美帆子	
	８６２２	９８４９	

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-297541

(43)Date of publication of application : 11.10.2002

---

(51)Int.Cl. G06F 15/00

G09C 1/00

---

(21)Application number : 2001-102393 (71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 30.03.2001 (72)Inventor : KUROKAWA KIYOSHI AZUMA SHOZO

SANO MUTSUO

---

(54) UNAUTHORIZED UTILIZATION NOTICE METHOD, ITS DEVICE AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an unauthorized utilization notice method, its device and program capable of monitoring unauthorized utilization for contents downloaded freely at a client-side without making a user be conscious.

SOLUTION: This method comprises: reading a hash value of contents described before the circulation from a contents ID attached to the contents after circulation (S10); calculating a hash value of contents for the contents after the circulation by using the same hash function as the hash function used in calculation of the hash value of contents described before the circulation (S40); determining whether the unauthorized utilization is present depending on whether the hash value of contents before-and-after the circulation are matched with each other (S50); and sending the unauthorized utilization information indicating the

unauthorized utilization in an address of a management server included in contents ID when the unauthorized utilization is present (step S60).

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The read-out step which reads the contents hash value described before circulation from the content ID which is the notice approach of unjust use which detects and notifies unjust use in the circulation process of the distributed contents, and is attached to the contents after circulation, The calculation step which computes a contents hash value using the same Hash Function as the Hash Function used for calculation of said contents hash value described before circulation to the contents after circulation, The decision step which judges whether there is any unjust use by whether both are in agreement to the contents hash value before and behind circulation, and when there is unjust use The notice approach of unjust use characterized by having the transmitting step which transmits the unjust use information which shows that the address of the management server contained in content ID had unjust use.

[Claim 2] The read-out means which reads the contents hash value described

before circulation from the content ID which is notice equipment of unjust use which detects and notifies unjust use in the circulation process of the distributed contents, and is attached to the contents after circulation, A calculation means to compute a contents hash value using the same Hash Function as the Hash Function used for calculation of said contents hash value described before circulation to the contents after circulation, A decision means to judge whether there is any unjust use by whether both are in agreement to the contents hash value before and behind circulation, and when there is unjust use Notice equipment of unjust use characterized by having a transmitting means to transmit the unjust use information which shows that the address of the management server contained in content ID had unjust use.

[Claim 3] It is the notice program of unjust use which detects and notifies unjust use in the circulation process of the distributed contents. The read-out step which reads the contents hash value described before circulation from the content ID attached to the contents after circulation, The calculation step which computes a contents hash value using the same Hash Function as the Hash Function used for calculation of said contents hash value described before circulation to the contents after circulation, The decision step which judges whether there is any unjust use by whether both are in agreement to the contents hash value before and behind circulation, and when there is unjust use

The notice program of unjust use characterized by having the transmitting step which transmits the unjust use information which shows that the address of the management server contained in content ID had unjust use.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention performs the circulation monitor of the contents which circulate extensively, and relates to the notice approach of unjust use and the notice equipment of unjust use which detect unjust use and notify unjust use information.

[0002]

[Description of the Prior Art] Bury beforehand the content ID which can identify contents uniquely, using a digital-watermarking technique as the conventional notice approach of unjust use to contents, it is made to set and circulate by **, and the network police technique of checking the correspondence relation between URL of a normal distribution place and the embedded content ID, and supervising unjust use with an unjust use detection system is known.

[0003] The following techniques are known as a detection technique used in such an unjust use detection system.

[0004] (1) The technique in which the retrieval robot which has a watermark reading function searches for the contents contained in the page of a website in top-down.

[0005] (2) The technique which checks all the contents that space through the gateway and server of a specific node which were prepared in the specific network, incorporate the reading filter, and pass this filter.

[0006] (3) It spaces through the download module of a user's browser, plug-in of the reading tool is carried out beforehand, and there is a bottom-up user cooperation mold which notifies and checks the content ID of contents and URL of an access site which were downloaded from the Web server in the content ID management center.

[0007] For example, the following services are offered in em ** (http://www.mken.co.jp/).

[0008] The yellow list round method which turns focusing on the website which took up with the search engine by making into a keyword the word which is likely to space and is likely to relate to entering contents with a watermark detection robot with this service, According to the gray list round method which turns focusing on a website with the possible contents of violation of copyright, the

Internet is always supervised for 24 hours, and the homepage in the world is patrolled. For example The contents which embedded digital watermarking of "acuaporta" are decoded and supervised, and it is striving for discovery of the contents which were copied, were altered unjustly and put up on the network.

[0009]

[Problem(s) to be Solved by the Invention] Thus, by the conventional notice approach of unjust use, it encapsulated with the protection-of-copyrights technique, and unjust use was prevented by attesting a key, a use condition, client information, etc. using the software of dedication. Moreover, the contents which have the misgiving of unjust use in a management server were transmitted, and digital watermarking currently beforehand embedded to contents was detected.

[0010] However, if it was in the conventional notice approach of unjust use, since the contents which have the misgiving of unjust use in a management server needed to be carried in, while the operation load of a management server increased with the spread of the Internet, there was a problem that extension of a management server was needed.

[0011] Then, the approach of detecting and notifying unjust use to the media player of the client side which reproduces contents has been searched for, without performing increase of the operation load of a management server,

extension of a management server, etc.

[0012] This invention was made in view of the above, and it is to the contents freely downloaded by the client side as the purpose to offer the notice approach of unjust use, the notice equipment of unjust use, and the notice equipment of unjust use which can supervise unjust use, without making a user conscious.

[0013]

[Means for Solving the Problem] In order that invention according to claim 1 may solve the above-mentioned technical problem, it is the notice approach of unjust use which detects and notifies unjust use in the circulation process of the distributed contents. The read-out step which reads the contents hash value described before circulation from the content ID attached to the contents after circulation, The calculation step which computes a contents hash value using the same Hash Function as the Hash Function used for calculation of said contents hash value described before circulation to the contents after circulation, The decision step which judges whether there is any unjust use by whether both are in agreement to the contents hash value before and behind circulation, and when there is unjust use Let it be a summary to have the transmitting step which transmits the unjust use information which shows that the address of the management server contained in content ID had unjust use.

[0014] In order that invention according to claim 2 may solve the

above-mentioned technical problem, it is notice equipment of unjust use which detects and notifies unjust use in the circulation process of the distributed contents. The read-out means which reads the contents hash value described before circulation from the content ID attached to the contents after circulation, A calculation means to compute a contents hash value using the same Hash Function as the Hash Function used for calculation of said contents hash value described before circulation to the contents after circulation, A decision means to judge whether there is any unjust use by whether both are in agreement to the contents hash value before and behind circulation, and when there is unjust use Let it be a summary to have a transmitting means to transmit the unjust use information which shows that the address of the management server contained in content ID had unjust use.

[0015] In order that invention according to claim 3 may solve the above-mentioned technical problem, it is the notice program of unjust use which detects and notifies unjust use in the circulation process of the distributed contents. The read-out step which reads the contents hash value described before circulation from the content ID attached to the contents after circulation, The calculation step which computes a contents hash value using the same Hash Function as the Hash Function used for calculation of said contents hash value described before circulation to the contents after circulation, The decision

step which judges whether there is any unjust use by whether both are in agreement to the contents hash value before and behind circulation, and when there is unjust use Let it be a summary to have the transmitting step which transmits the unjust use information which shows that the address of the management server contained in content ID had unjust use.

[0016]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to a drawing.

[0017] Drawing 1 is drawing showing the configuration of the DRM processing flow which can apply the notice approach of unjust use concerning the gestalt of 1 operation of this invention.

[0018] As shown in drawing 1 , the media player 23 for reproducing the media server 21 for distributing the DRM (Digital Rights Management) equipment 17 for managing the encoder equipment 13 for creating contents and contents and contents and contents is formed in this system.

[0019] It has the function changed into the file into which encoder equipment 13 was generally called the encoder, inputted the media files A11, such as screen information of the live image from a camera, a multimedia file, and a client (personal computer), it encoded according to the fixed regulation, and the assignment format was compressed, and the changed media file B15 is

outputted.

[0020] DRM equipment 17 consists of a Web server, the menu page of a website and the registration page to which demand of information or payment is performed are offered, and it has the function to give the license key for defrosting etc. from a registration page. License management and a copyright function manager for especially DRM equipment 17 to protect contents are performing contents management. Add the URL information for inputting the media file B15 changed by encoder equipment 13, and acquiring a key number and a license, and the media file B15 is received. It encapsulates so that it may encipher using the key number which can perform inverse transformation of conversion by encoder equipment 13, and license acquisition URL information and may become data of one, and this encapsulated media file C19 is transmitted to the media server 21. In addition, the encapsulated media file 19 is protected so that the inverse transformation mentioned above if it was enciphered with the license and a "key" was not used may be impossible. This "key" is separately distributed to the media player 23 from DRM equipment 17.

[0021] Moreover, in order to make a user download the encapsulated media file 19, put on the website on a server, or it places on the media server 21 for streaming, or CD-ROM is distributed as a medium.

[0022] The media player 23 is supporting communication facility with DRM

equipment 17. For example, the media file C19 encapsulated from the media server 21 is downloaded. Extract the key number and content ID which were extracted from the media file C19, and it transmits to DRM equipment 17. Certificates, such as this key number, a key corresponding to content ID, use conditions, and client information, are answered from DRM equipment 17. Inverse transformation of the encapsulated media file C19 is carried out to the media file 25, and the media file 25 is reproduced by the decoding function according to the use conditions included in the license. In addition, use conditions with start time, a date, a period, the count of playback, etc. being various for carrying out the exercise can be given to a license.

[0023] Moreover, in order to reproduce the protected media file C19, a user needs to acquire the license key for carrying out inverse transformation of the media file C19 to the media file B15 first. The acquisition timing of a license key is automatically started, when it tries to acquire the media contents C19 from which the user was protected, or when a media file is reproduced for the first time.

[0024] At this time, DRM equipment 17 will guide a user to the registration page on the website to which demand of information or payment is performed from the menu page of a website, and a user will acquire the license key for defrosting from on the guided registration page.

[0025] Moreover, the media player 23 checks whether sequential reference of the media file based on the content ID on the client (personal computer) in which this media player 23 exists is carried out, and the unjust use check flow mentioned later has unjust use of the media file of a twist, while reproducing the media file C19.

[0026] Next, drawing 2 is an explanatory view shown in the detailed configuration of content ID.

[0027] As shown in drawing 2 , in detail to content ID As an identifier uniquely given to contents since the attribute information about contents is specified ID center management number which expresses the number (unique code) given to contents at a meaning from left-hand side, The contents attribute showing the information about the creator and the contents of contents, classification, a classification, etc., The right attribute which writes the right relation of contents, the right employment attribute showing the information about consent, election, and a check of a right, The system area showing the free field and digital signature showing the circulation attribute showing the hysteresis information on circulation (= dealing) of contents, the distribution attribute showing the information about distribution of a dealing profit, and the free field left to ID management center, a contents hash value, etc. is set up.

[0028] Furthermore, there is information about systems, such as a method of the

information for specifying contents, the information about circulation, and digital watermarking, in the component of content ID. There is a unique code and circulation descriptor (DCD:Distributed ContentDescription) in these expression approaches, and it uses properly if needed. In addition, circulation descriptors (DCD) are critical information, such as use conditions beforehand specified by the rightful claimant in content ID.

[0029] Among these, as shown in drawing 3 , the digital signature and contents hash value for bundling contents and content ID (circulation descriptor: DCD) are contained, and an unjust check is performed in a system area using these. Furthermore, there are a link to the contents for connecting with contents data, digital-watermarking information, signature algorithm information, a check digit, etc. in a system area.

[0030] Here, the DS and the mathematical description of a digital signature and a contents hash value are explained, and it explains how an unjust check is performed.

[0031] As shown in drawing 3 , in the digital signature based on a public key cryptosystem, the contents (electronic filing document) from which a signature implementer becomes the contents of a communication link are enciphered with the signature key (private key) of a signer proper, and it has become the structure that it is verifiable with the verification key (public key) of the signature

implementer corresponding to the signature key in the addressee of contents with a signature (electronic filing document) whether it is that the digital signature is a signature of a transmitting person truly.

[0032] Therefore, a digital signature has the advantage that the fact of having been altered is also verifiable with the verification process of the signature mentioned later, if the affinity of the signature itself and the electronic filing document itself which is the contents of a communication link is strong and the contents of a communication link are altered on the way of [a communication link] from the technical property of considering as a signature what enciphered the contents of a communication link.

[0033] As shown in drawing 3 , contents data and a digital signature are separated, and the clear digital signature (separation signature) which is one of the concrete implementation approaches can read contents data as it is, and, on the other hand, contains the contents hash value (value calculated in the secret formula) of the contents text in the system area where the digital signature is described.

[0034] For this reason, when a digital signature is altered, the contents hash value set as the signature object of a digital signature will also be altered by coincidence. Consequently, an actual contents hash value is calculated, the calculated contents hash value differs from the contents hash value in content ID,

and the alteration of a digital signature can be detected.

[0035] The contents hash value shown in drawing 3 here is a value acquired by the Hash Function decided beforehand, and since it contains an irreversible one-way function in a Hash Function, it is very difficult to create different contents data which cannot reproduce contents data from a contents hash value, and have the same contents hash value to it. In addition, as a Hash Function, MD5, SHA1, etc. are known widely, for example.

[0036] In a concrete detection process, moreover, this Hash Function It is the operation technique which generates a fixed-length pseudo-random number from the given contents data. In case contents data are offered through circulation processes, such as a communication link, the contents hash value which used and asked for the Hash Function from the contents data before circulation is extracted from the system area of content ID. If it compares with the contents hash value calculated using the Hash Function from the contents data after circulation, it can investigate whether contents data are in the middle of communicative circulation, and are altered.

[0037] Next, drawing 4 is the embedding flow of the content ID in the creation time of contents.

[0038] As shown in drawing 4 , there are identifiers, such as WAV.WMA.MP3, about a voice file as a media file A11, there are identifiers, such as

WMV.ASF.AVL.MPEG1, about an image file, and there is BMP as an identifier of other files. The media file A11 can treat 2 hierarchy digital watermarking as an option.

[0039] As a media file B15 changed with encoder equipment 13, there are identifiers, such as WMA, WMV, and ASF, and DCD mentioned above to the header information of these encapsulated media files B15 is embedded.

[0040] The media file C19 encapsulated with DRM equipment 17 binds DCD mentioned above.

[0041] In addition, the media file A11 can treat as an option first-floor layer digital watermarking using the unique code which consists of an ID center management number.

[0042] Here, first-floor layer digital watermarking which embeds two kinds of different digital watermarking one by one is explained.

[0043] At digital watermarking, since there is a possibility that detection time may become huge when there are many methods and all digital watermarking is tried one by one, the classification information on real digital watermarking is embedded using meta-digital watermarking. This real digital watermarking embeds the management number of ID center, and meta-digital watermarking embeds the classification information on a real watermark.

[0044] Since a detection procedure detects the real watermark which specified

the classification of real digital watermarking by detection of meta-digital watermarking, and was specified further, it can complicate the detection process of the unique code embedded by two kinds of different digital watermarking, and the easy decode by the inaccurate user can be prevented from the ability doing.

[0045] In addition, the unique code shows ID center management number, and the configuration is as follows.

[0046] (1) Area code (4 bits)

The world is divided into 16 areas and numbering of a center is possible.

[0047] (2) Center number (8 bits)

Registoration Authority It is the number of the fixed length who publishes and identifies ID center.

[0048] (3) The number in a center (arbitration)

It is the number which identifies the contents which ID center manages, and ID center assigns to arbitration.

[0049] (4) Version number (4 bits)

It is the number which specified the version of content ID using the binary expression by the binary number.

[0050] Next, drawing 5 is drawing showing the functional configuration of the media player 23.

[0051] The media player 23 carries out the sequential check of the file based on

the content ID on the client to which the media player 23 exists during playback of the media file 25, and checks the media file of unjust use.

[0052] An example of the functional configuration of the media player 23 is shown in drawing 5 . The media player 23 consists of the authentication section 41, the circulation information storage section 43, the unjust use check section 45, and the media playback section 47.

[0053] Moreover, the media file reproduced by the media player 23 has header information, the systematization field, the digital signature, the contents hash value, and the contents field from the head.

[0054] The authentication section 41 extracts a key number and content ID from the inputted media file, transmits to DRM equipment 17, and attests by receiving certificates, such as a key, a use condition, and client information, from DRM equipment 17.

[0055] The circulation information storage section 43 accumulates the circulation attribute collected from the content ID of the media file reproduced in the past as circulation information.

[0056] The unjust use check section 45 is a module which searchs the media file on a client and detects unjust use, and is processed by the unjust use check flow which shows the detailed actuation to drawing 6 .

[0057] The media playback section 47 reproduces the media file 25 by the

decoding function according to the use conditions received from DRM equipment 17. This decoding function is a function which decodes the encoded media file 25 to the media file A11 contrary to coding by encoder equipment 13.

[0058] Here, the fundamental actuation by the media player 23 shown in drawing 5 is explained.

[0059] In addition, RAM which memorizes OS program, control data, and an application program temporarily, and CPU which controls a system according to a control program or an application program are prepared in the control section at the client which consists of a personal computer. Moreover, the application program currently recorded on the hard disk HD is a program installed from record media, such as CD-ROM, using the CD-ROM drive formed in the personal computer, and is the record medium which recorded the notice program of unjust use of this invention.

[0060] URL of the media server 21 is specified from the screen of the media player 23 on a client, a homepage is opened, and a media file is received. And in the authentication section 41, a key number and content ID are extracted from the inputted media file, and it transmits to DRM equipment 17. And the authentication section 41 attests by receiving certificates, such as a key, a use condition, and client information, from DRM equipment 17. And in the media playback section 47, the media file 25 is decoded to the media file A11 according

to use conditions, such as the start time and the date which received from DRM equipment 17, a period, and a count of playback, and it reproduces.

[0061] In parallel to the time of reproducing the media file in this media playback section 47, the unjust use check section 45 performs the unjust use check for other media files which are on a client in the background.

[0062] In drawing 6 , if an unjust use check is started, at step S10, header information will be read from the content ID of the media file 25, and the contents hash value and digital signature which were described before circulation will be read from the content ID especially attached to the media file after circulation.

[0063] And alteration check processing of a digital signature is performed at step S20.

[0064] That is, the contents hash value after circulation is calculated using the same Hash Function as the Hash Function used for calculation of the contents hash value described before circulation, and when the contents hash values before the circulation described in the contents hash value after the calculated circulation and content ID differ, it means that there had been an alteration of a digital signature.

[0065] And at step S30, it judges whether there is any alteration. When there is no alteration, it progresses to step S40 and the contents hash value after circulation is computed using the same Hash Function as the Hash Function

used for calculation of the contents hash value described before circulation to the contents after circulation.

[0066] And at step S50, the contents hash value after the computed circulation judges whether it is the contents hash value and inequality before the circulation read from the content ID of the media file 25.

[0067] Here, since it is shown that it is normal use when the contents hash value after the computed circulation is in agreement with the contents hash value before circulation of the media file 25, processing is ended as it is.

[0068] When it is judged on the other hand that there is an alteration at step S30, or when the contents hash values before and behind circulation are inequalities at step S50, it progresses to step S60, the unjust use information which shows that the address of the management server contained in content ID had unjust use is transmitted, and processing is ended.

[0069] Thus, in the unjust use check section 45, since the check of the digital signature of the media file 25 and a contents hash value is performed, the media file 25 concerned can detect whether it is unjust use, and when the media file 25 concerned is unjust use, the unjust use information which shows that the address of the management server contained in content ID had unjust use can be transmitted.

[0070] Moreover, the unjust use information which shows that the center

address (URL of a center server) shown in content ID had unjust use can be notified. In addition, suppose that content ID, an existence location (IP address of a terminal), and an unjust use check result are included in this unjust use information.

[0071] Consequently, unjust use can be supervised to the contents downloaded freely, without making a user conscious, and it can apply to a media player especially. Moreover, it is applicable as an unjust monitor means of a client side.

[0072] Moreover, even when a new digital signature method and a new check item are added according to version up of a media player, an unjust use detection flow can be reformed easily.

[0073] The effectiveness in the gestalt of this operation reads the contents hash value described before circulation from the content ID attached to the contents after circulation. The contents hash value is computed using the same Hash Function as the Hash Function used for calculation of said contents hash value described before circulation to the contents after circulation. When it judges whether there is any unjust use by whether both are in agreement to the contents hash value before and behind circulation and there is unjust use Unjust use can be supervised without making a user conscious by transmitting the unjust use information which shows that the address of the management server contained in content ID had unjust use to the contents downloaded freely.

[0074]

[Effect of the Invention] According to this invention according to claim 1 to 3, the contents hash value described before circulation is read from the content ID attached to the contents after circulation. The contents hash value is computed using the same Hash Function as the Hash Function used for calculation of said contents hash value described before circulation to the contents after circulation. When it judges whether there is any unjust use by whether both are in agreement to the contents hash value before and behind circulation and there is unjust use Unjust use can be supervised without making a user conscious by transmitting the unjust use information which shows that the address of the management server contained in content ID had unjust use to the contents downloaded freely.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the DRM processing flow which can apply the notice approach of unjust use concerning the gestalt of 1 operation of this invention.

[Drawing 2] It is the explanatory view shown in the detailed configuration of content ID.

[Drawing 3] It is the explanatory view shown in the detailed configuration of DCD.

[Drawing 4] It is the embedding flow of the content ID of contents creation time.

[Drawing 5] It is drawing showing the functional configuration of the media player 23.

[Drawing 6] It is a flow for explaining detailed actuation of the unjust use check section 45.

[Description of Notations]

13 Encoder Equipment

17 DRM Equipment 17

21 Media Server

23 Media Player

25 Media File

31 Content ID

41 Authentication Section

43 Circulation Information Storage Section

45 Unjust Use Check Section

47 Media Playback Section

－３０，３２に係る発明は、引用例１に記載された発明に、引用例２のＲＯＭメディアで提供する技術、再生だけではなくコピー制御の著作権管理をする技術、利用形態も送信する技術を必要に応じてそれぞれ適用し、当業者が容易に成し得たものである。

・請求項　９，１８，２５，３１
・引用例　１－４
・備考
　引用例３の第００２０段落又は引用例４の００２２段落には、鍵データにコンテンツに対する利用権情報を付加して送信する技術について記載されている。
　引用例１－４は全てコンテンツの著作権管理に関する共通の技術分野に属する。
　したがって、本願請求項９，１８，２５，３１に係る発明は、引用例１に記載の発明において鍵データを送信する際に、引用例３又は引用例４の鍵データに利用権を付加して送信する技術を適用し、必要に応じて引用例２に記載されたそれぞれの技術を適宜、引用例１に適用し、当業者が容易に成し得るものである。

・請求項　１４－１５
・引用例　１，５
・備考
　引用例１には、媒体購入時に利用権（再生条件）を設定する技術と、さらに、利用権を媒体識別情報と共にサーバに送信する技術についても記載されている。
　また、利用権を媒体購入時に設定する際に、媒体購入店における端末を使用するようにすることは、当業者であれば適宜設計可能な事項である。
　引用例５には、ＲＯＭメディア購入時に店舗端末を使って媒体ＩＤをサーバに送信する技術について記載されている。（第９頁第３８行目－第４４行目参照）
　引用例１，５は共にコンテンツの著作権管理に関する共通の技術分野に属する。
　したがって、本願請求項１４－１５に係る発明は、引用例１の媒体入手時に、引用例５のＲＯＭ媒体入手時に店舗端末から媒体識別情報をサーバに送信する技術を適用し、当業者が容易に成し得たものである。

引　用　文　献　等　一　覧
１．特開２００２－２９７４５３号公報
２．特開２０００－１９６５８５号公報
３．特開２００１－２０９５８６号公報

４．特開２００２－２９７５４１号公報
５．国際公開第０２／０５２４７３号

理由２
　この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第２号に規定する要件を満たしていない。

記

・請求項　６

・備考
「該利用の形態」と記載されているが、利用の形態は前記されておらず、どの利用の形態を指しているのかわからない。

・請求項　２６－３２
・備考
「再生および／または記録制御装置」との記載は、再生制御装置、記録制御装置、記録再生制御装置のうち、どの制御装置の発明と特定してよいのかわからない。
よって、請求項６，２６－３２に係る発明は明確でない。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

先行技術文献調査結果の記録

・調査した分野　　ＩＰＣ第７版　Ｇ１１Ｂ２０／１０
Ｇ０６Ｆ１２／１４
Ｇ０６Ｆ　３／０６
Ｈ０４Ｌ　９／００

この先行技術文献調査結果の記録は、拒絶理由を構成するものではありません。

この拒絶理由通知の内容に関するお問い合わせ、または面接のご希望がございましたら下記までご連絡下さい。

特許審査第四部データ記録　高野　美帆子
TEL. 03(3581)1101 内線3589～3591
FAX. 03(3580)6906

部長／代理	審査長／代理	審査官	審査官補
	渡邊　聡	高野　美帆子	
	８６２２	９８４９	

拒絶理由通知書

特許出願の番号	特願２００２－３２１３５９
起案日	平成１８年　７月３１日
特許庁審査官	高野　美帆子　　９８４９　５Ｑ００
特許出願人代理人	杉浦　正知（外　１名）　様
適用条文	第２９条第２項、第３６条

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

理由１

この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　　（引用文献等については引用文献等一覧参照）

・請求項　１－８，１０－１３，１６－１７，１９－２４，２６－３０，３２
・引用例　１－２
・備考

引用例１には、ＲＯＭ領域にコンテンツデータが記録された媒体の媒体識別情報と媒体の管理情報とを関連づけてサーバに記憶させ、記録媒体に記録された媒体識別情報を読み出してネットワークを介して送信し、受信された媒体識別情報から媒体の管理情報を読み出して管理情報に基づいてコンテンツの再生を可能にする鍵を発行してネットワークを介して端末側に送信し、管理情報に応じたサービスを提供し、利用形態に応じて管理情報を書き換えるシステムについて記載されており、管理情報は利用可能情報（再生条件）である再生可能回数及び再生有効期限を含み、利用可能情報（再生条件）はディスク販売時（ユーザに入手される時）に設定可能であることについても記載されている。

引用例２には、暗号化された超流通コンテンツの著作権管理に関して、コンテンツをＲＯＭメディアで提供する技術、著作権管理を再生又は他の媒体へのコピーの制御において行う技術、再生かコピー（買い取り）かの利用形態を示す課金情報を送信する技術について記載されている。

引用例１と２は共にコンテンツの著作権管理に関する共通の技術分野に属する。

したがって、本願請求項１－８，１０－１３，１６－１７，１９－２４，２６